



# **DISN Video Services (DVS) Customer Connection**

---

## **Approvals**

**DVS Information Assurance Support**

**April 2009**



# Agenda

---

- **Purpose**
- **Customer Configurations**
- **Connection Approvals**





# Purpose

- **Present approved customer configurations and IA controls**
  - Video IP Network
  - Dial-up Connection
  - Hybrid Connection
  - Periods Processing
  - Non Open Storage VTC Facility
  - Available Products
- **Identify required connection approvals to access DVS**
  - Order Transmission Paths
  - Register CODEC on PPSM
  - DSN Certification
  - Video Teleconferencing (VTC) System Certification and Accreditation (C&A)
  - SIPRNet Connection Approval
  - NIPRNet Connection Approval
  - DSN Connection Approval
  - DVS Connection Approval





# Customer Configurations

## • Video IP Network Minimum Requirements

- Dedicated video network separate from the data network, e.g. video VLAN
- Network protection consisting of Router with ACL, H.323 aware Firewall, and Intrusion Detection System (IDS)
- Approved Ethernet A/B switch for switching between Classified and Unclassified networks
- External indicators of secure/non-secure connection status
- Fiber Optic Modem (FOM)/Transceiver powered-off in the path that is not used
- Periods processing procedures to remove residual information when switching devices between classification levels
- H.323 CODEC

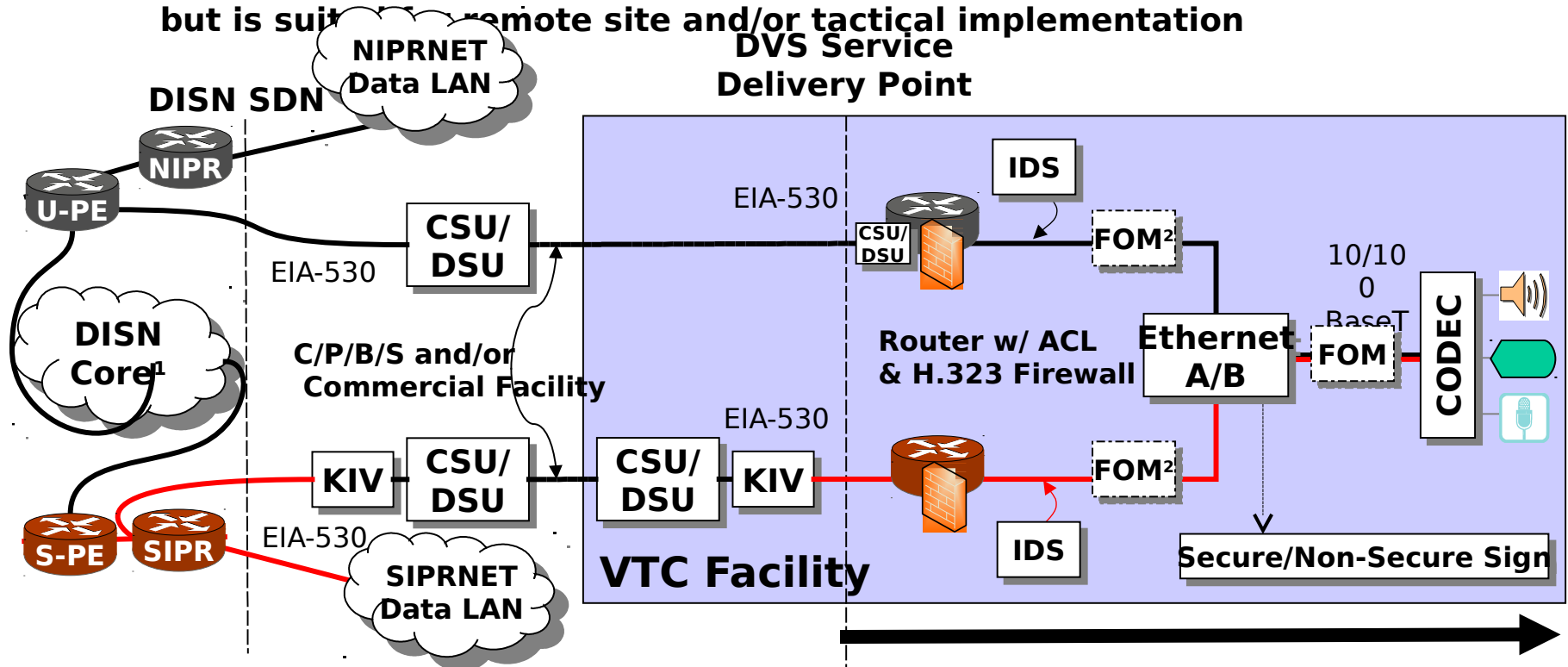




# Customer Configurations

- **Option 1 - Classified/Unclassified Single Facility Direct IP Connection**

- Originally designed to quickly transition dedicated DVS-G sites to DVS-II, but is suitable for remote site and/or tactical implementation
- DVS Service Delivery Point**



- 1 Or Customer WAN with QoS and connection to DISN
- 2 Fiber Optic Modem (FOM)/Transceiver powered-off in the path that is not used

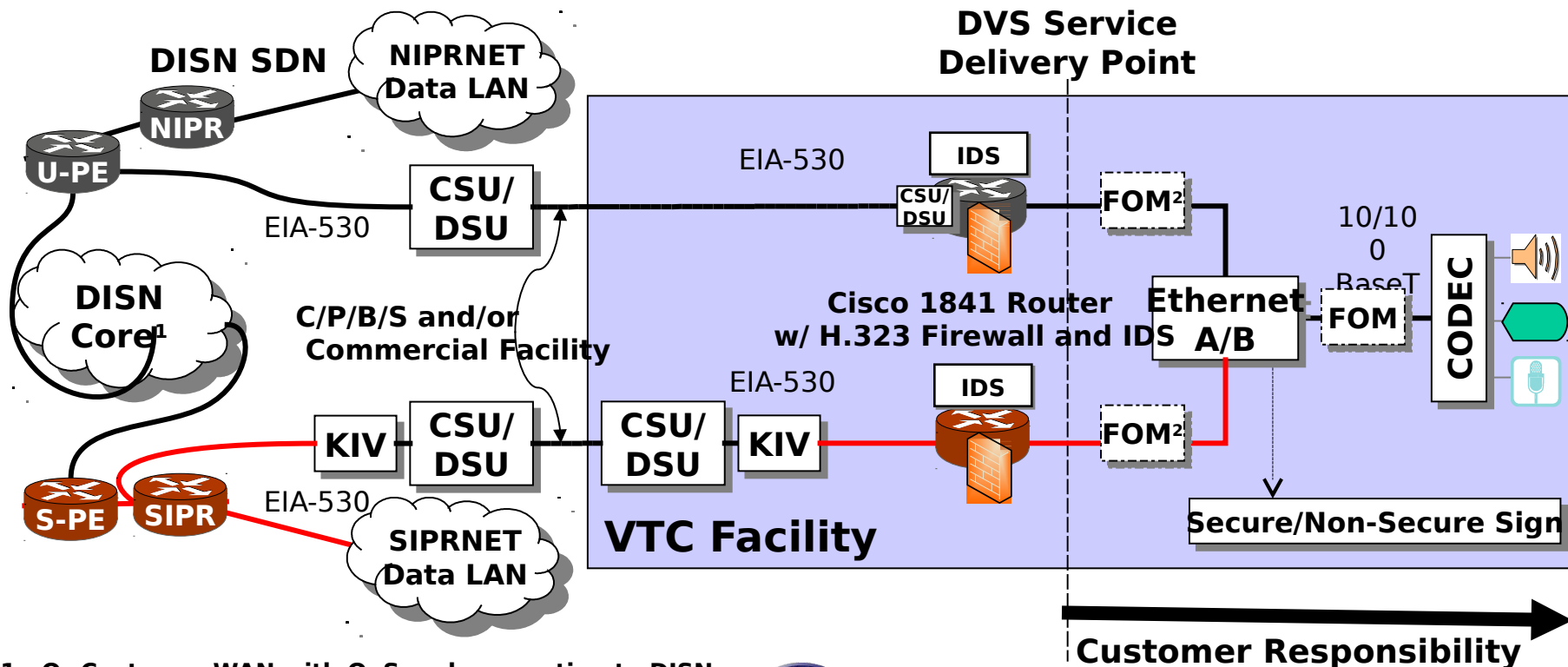




# Option 1x Customer Configuration

- **Option 1x - Classified/Unclassified Single Facility Direct IP Connection for transitioning dedicated DVS-G Customers**

- **H.323 aware IOS Firewall within the Cisco 1841 must be enabled by January 2009 and customer purchased AIM IDS Module must be enabled by January 2010**
- **DISA CONUS will manage the Cisco 1841 until January 2011, after which, the customer has an option to take over management or continue with DISA for a monthly fee TBD**



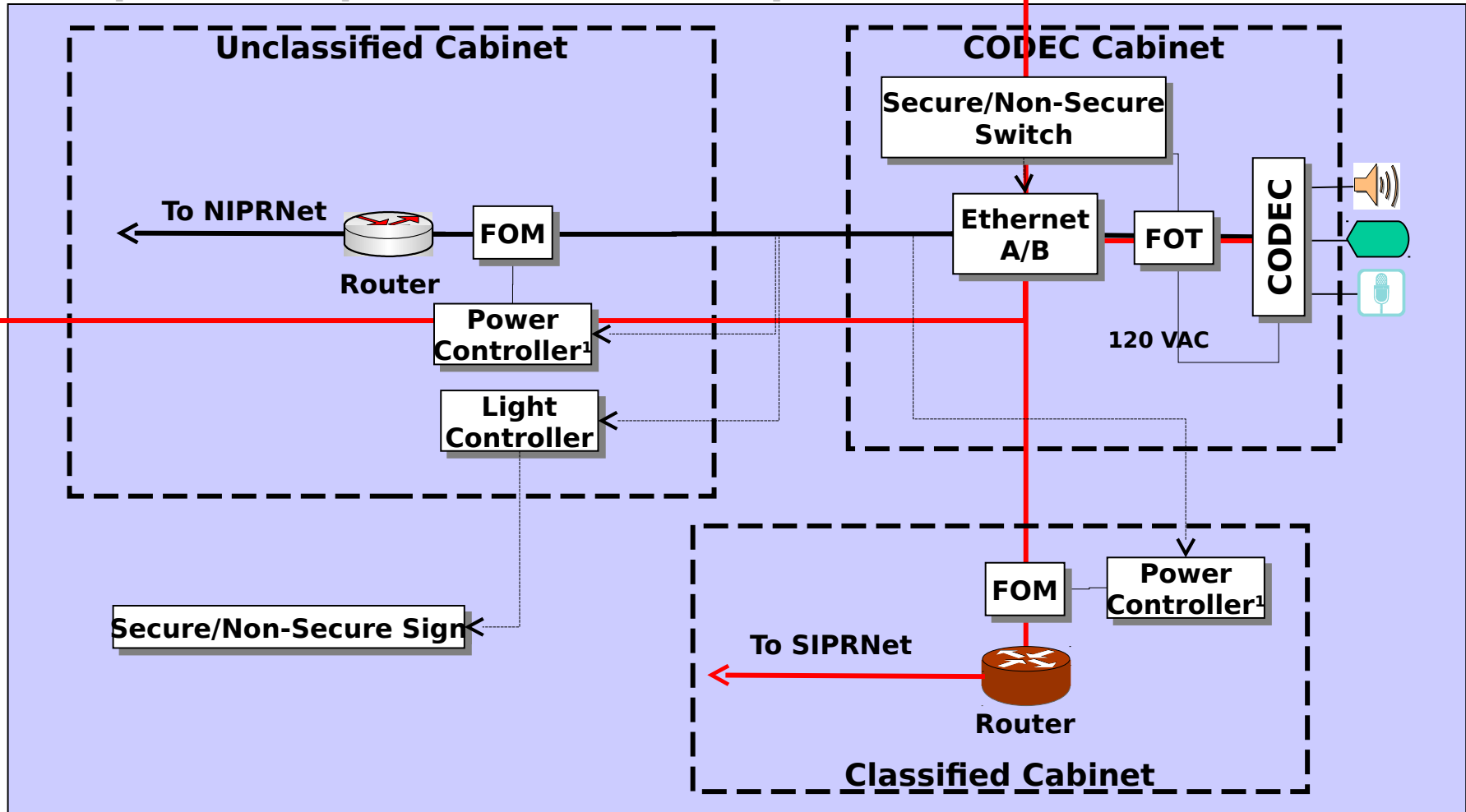
- 2 **Fiber Optic Modem (FOM)/Transceiver**





# Customer Configurations

## • Option 1 Implementation Example



1 Powers off Fiber Optic Modem (FOM) in the path that is not used



- **For campus and implementation with multiple VTC facilities**

- For campus and service provider implementation with multiple VTC facilities

**DISN SDN**

The diagram illustrates a network architecture for DISN SDN, divided into two main sections by a vertical dashed line. On the left, the 'DISN Core' contains two sets of edge routers: 'U-PE' and 'NIPR' at the top, and 'S-PE' and 'SIPR' at the bottom. On the right, the 'Customer' section contains two identical network stacks. Each stack includes a 'CE Router' connected to an 'ACL' (Access Control List) and an 'IDS' (Intrusion Detection System). The top stack is connected to 'NIPRNET Data LAN' and 'NIPRNET Video VLAN'. The bottom stack is connected to 'SIPRNET Data LAN' and 'SIPRNET Video VLAN'. A 'H.323 Firewall' is positioned between the two stacks. The 'Customer' section also includes 'Ethernet A/B' and 'FOM' (Facility Onboard Module) components, which are connected to a 'CODEC' and a 'Secure/Non-Secure Sign' block. A large double-headed arrow at the bottom indicates the 'Customer' interface.

U-PE NIPR

DISN Core<sup>1</sup>

S-PE SIPR

CE Router

ACL

IDS<sup>3</sup>

NIPRNET Data LAN

NIPRNET Video VLAN

H.323 Firewall<sup>2</sup>

SIPRNET Data LAN

SIPRNET Video VLAN

Ethernet A/B

FOM<sup>4</sup>

Secure/Non-Secure Sign

10/10 0 BaseT

CODEC

Multiple VTC Facilities

Customer

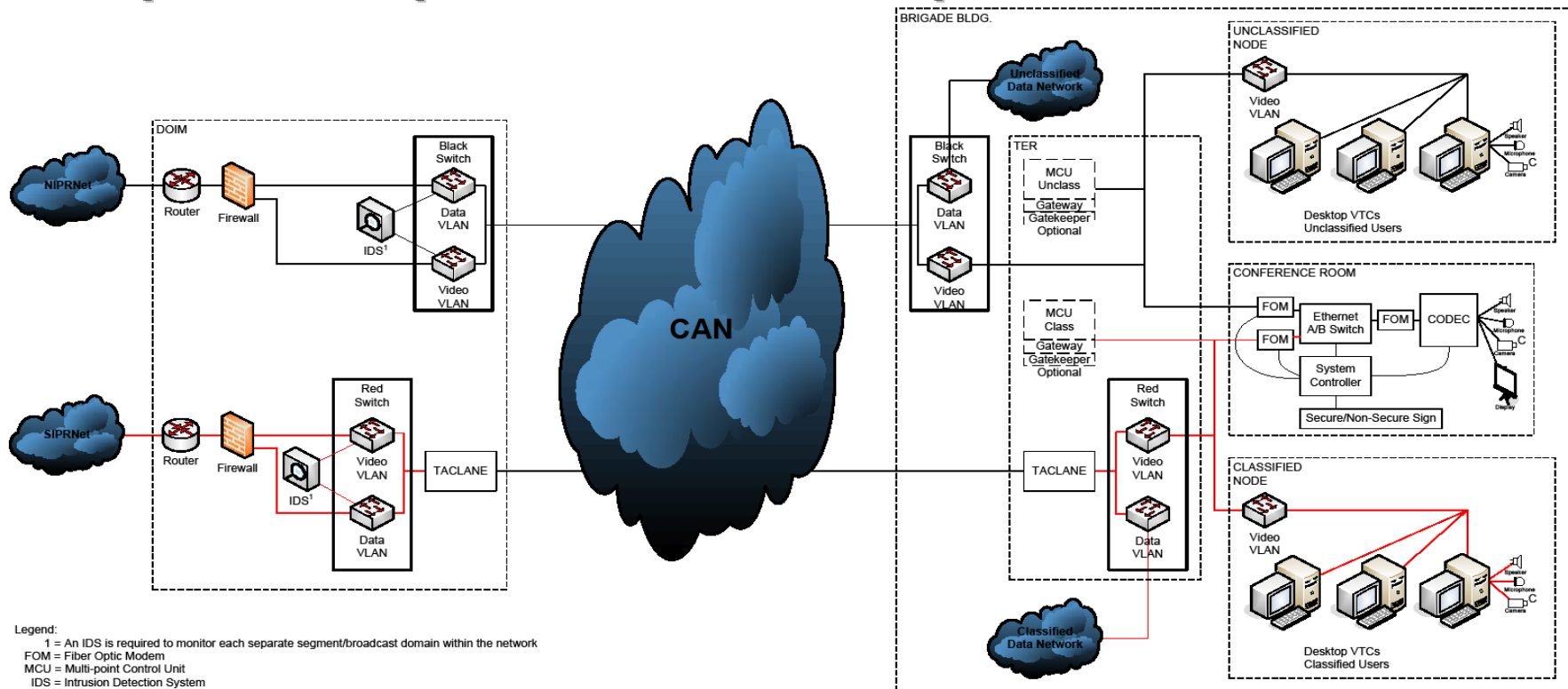
## Customer Responsibility

**4 Fiber Optic Modem (FOM)/Transceiver powered-off in the path that is not used**



# Customer Configurations

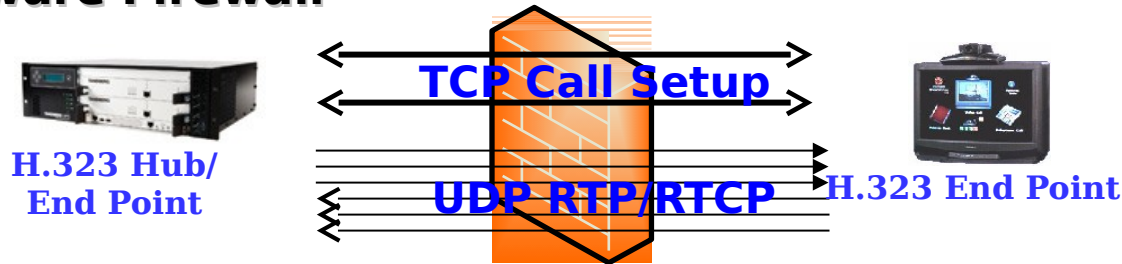
## • Option 2 Implementation Example





# Customer Configurations

- **H.323 Aware Firewall**



- Understands the H.323 protocol and dynamically open the ports needed by the video session and closes them when the session is over
- H.323 Ports
  - 1718 UDP - H.225.0 Gatekeeper Discovery
  - 1719 UDP - H.225.0 Gatekeeper RAS
  - 1720 TCP - H.225.0 Call Signaling
  - 1025-65535 Dynamic TCP - H.245 Media Control
  - Even-numbered ports above 1024 UDP - RTP (Media Stream)
  - Next corresponding odd-numbered ports above 1024 UDP - RTCP (Control Information)
- Gatekeeper Name Resolution
  - 53 TCP/UDP - DNS Lookup

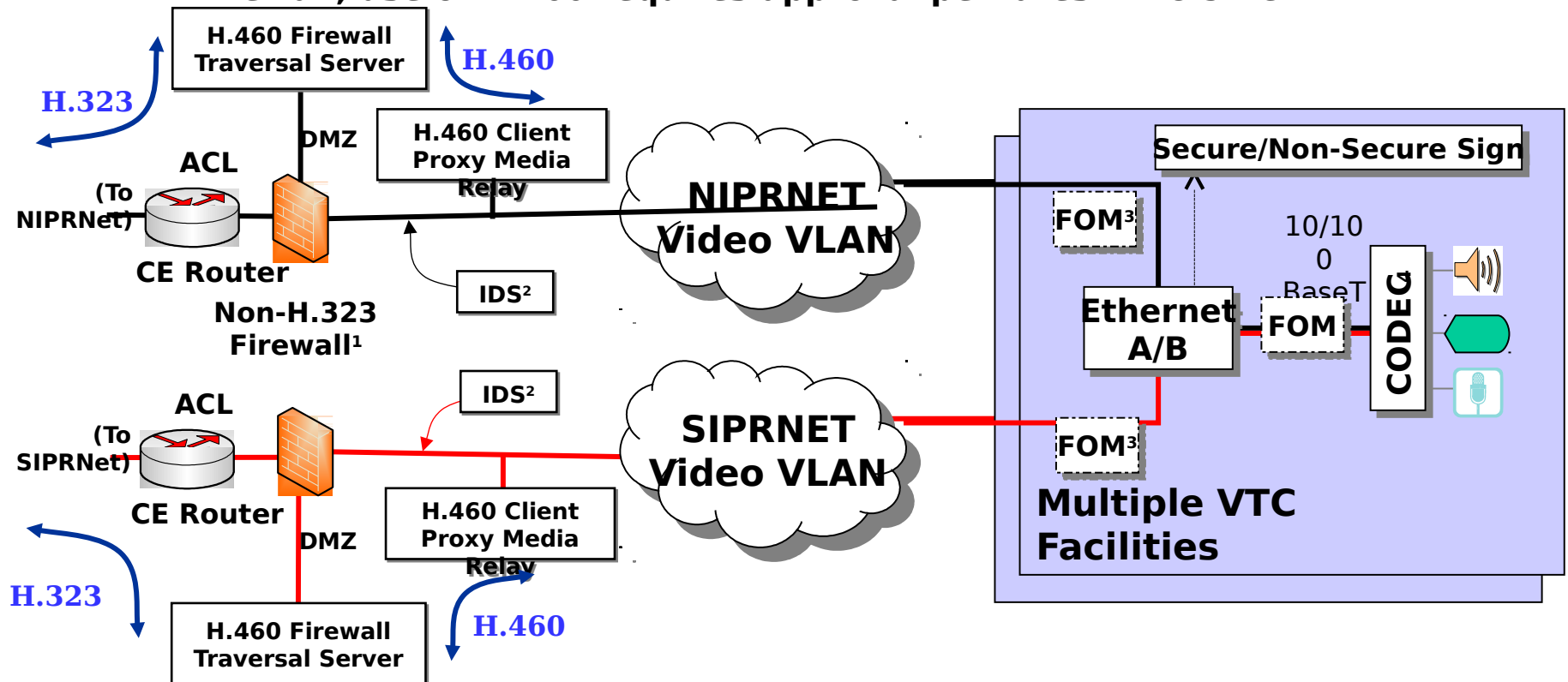




# Customer Configurations

## • H.460 Firewall Traversal

- For customers doing video now and cannot upgrade to an H.323 aware Firewall; use of H.460 requires approval per latest VTC STIG



- 1 The same Firewall could be used for both video and data provided it has the required performance
- 2 IDS to monitor each network segment IAW the Network STIG

- 3 Fiber Optic Modem (FOM)/Transceiver powered-off in the path that is not used
- 4 Non-H.460 aware CODECs need to go via the H.460 Client Proxy Media Relay to traverse the Firewall



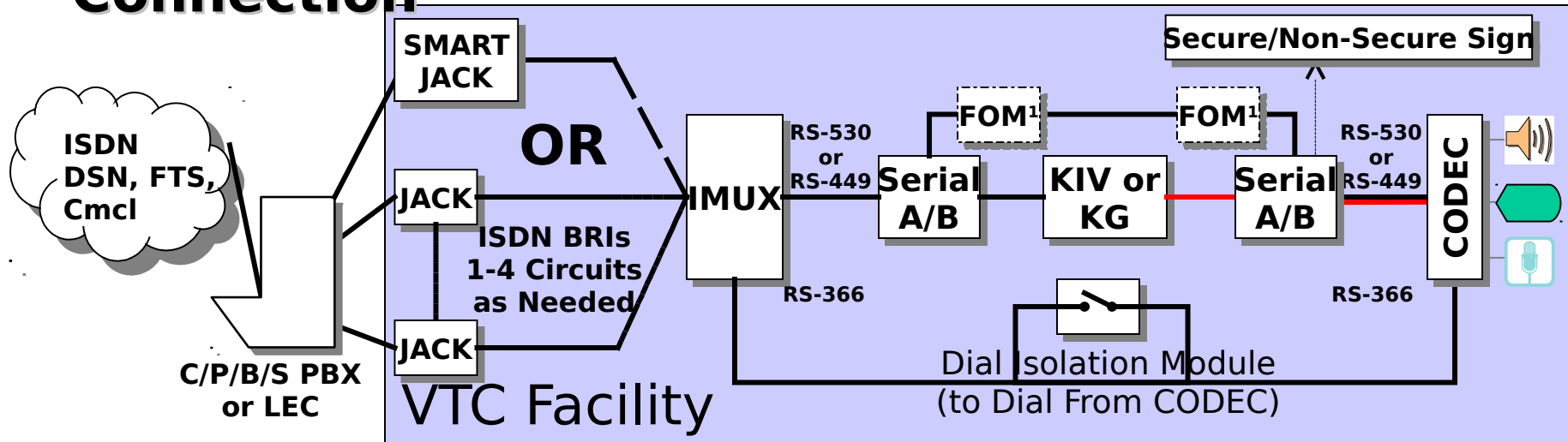
# Customer Configurations

- **Dial-up Connection Minimum Requirements**
  - **DSN Certified hardware and/or software for sending and receiving voice, data or video signals, e.g. IMUX, CODEC**
  - **Tempest 2/95-A compliant Serial A/B switches and/or Fiber Optic Modems for Red/Black isolation**
  - **Dial isolator to dial from the CODEC**
  - **Type 1 encryption for classified connection**
  - **External indicators of secure/non-secure status**
  - **Periods processing procedures to remove residual information when switching devices between classification levels**
  - **H.320 CODEC**



# Customer Configurations

- **Option 3 - Classified/Unclassified Dial-up Connection**

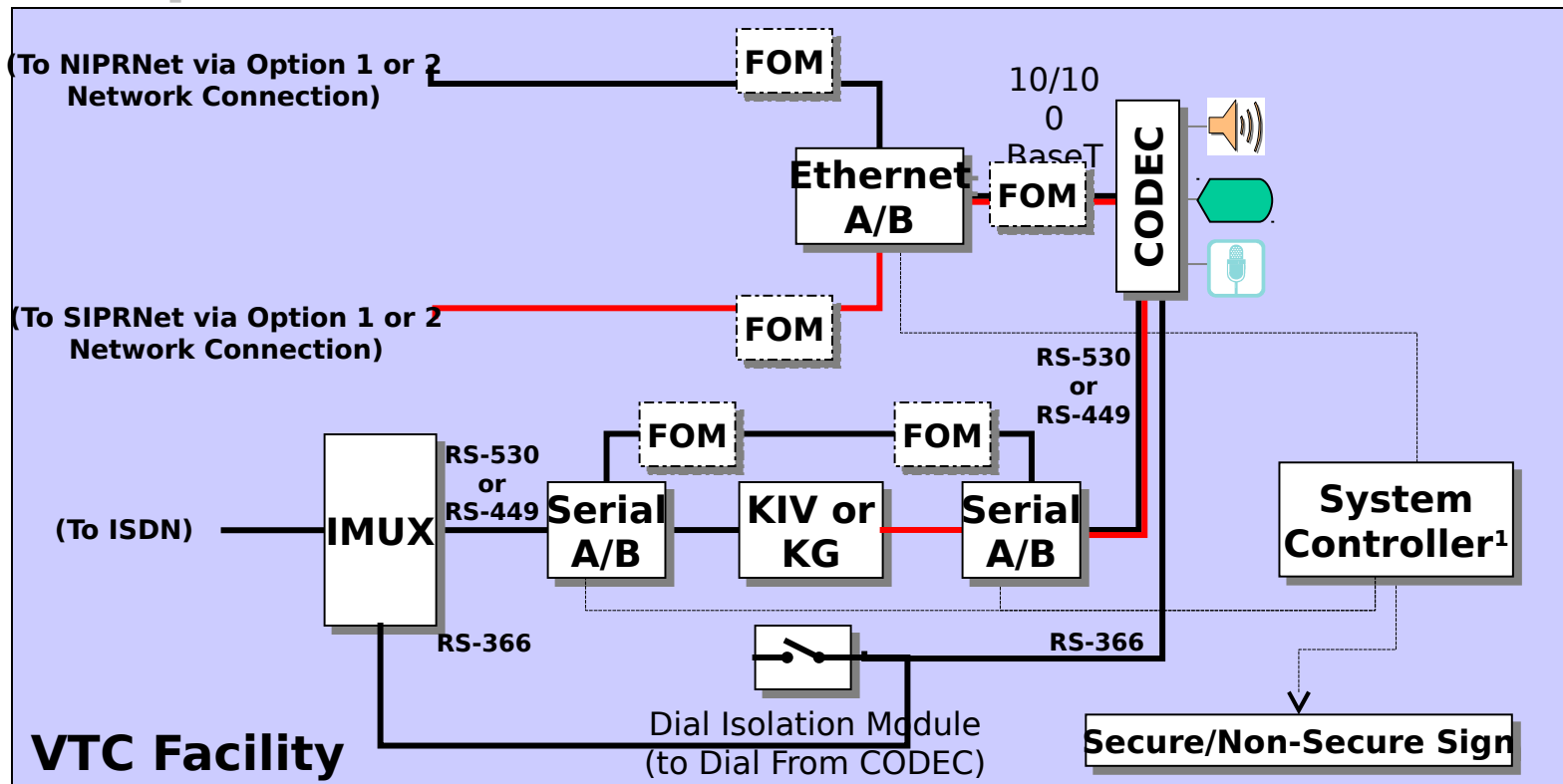


- 1 Fiber Optic Modem (FOM)/Transceiver powered-off in the path that is not used in lieu of Red/Black isolation within the Serial A/B switch



# Customer Configurations

- **Option 4 - Classified/Unclassified Hybrid IP and Dial-up Connections**

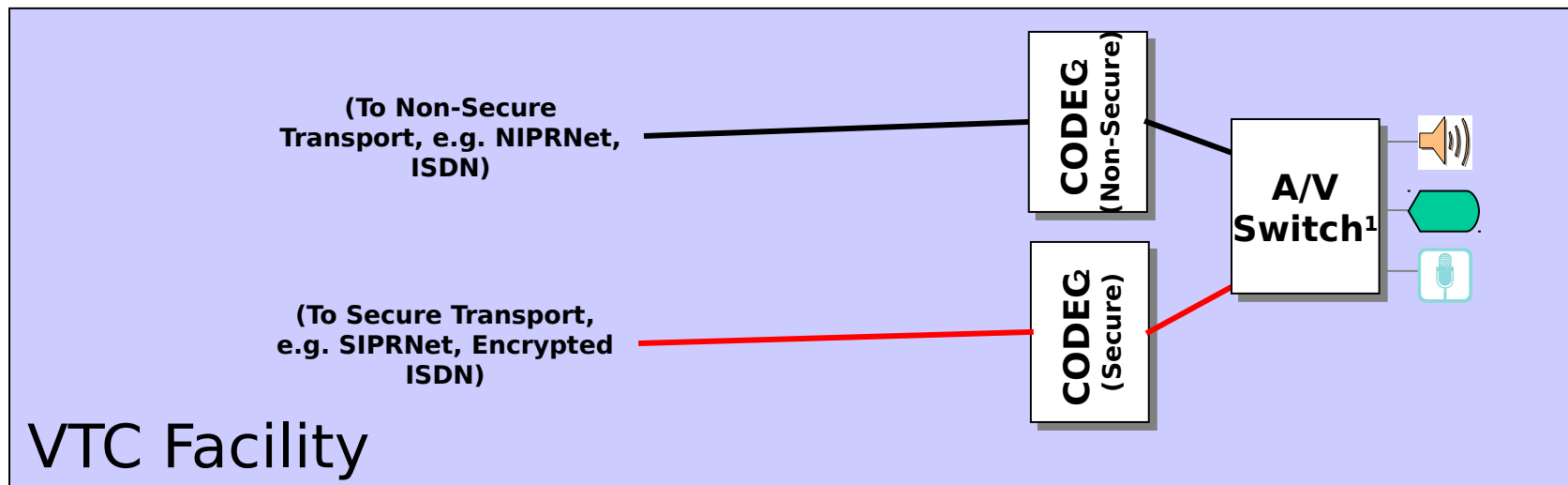


- 1 A/B Switches centrally controlled to ensure that both IP and Dial-up connections are at the same classification level



# Customer Configurations

- **Dual CODECs solution in conjunction with approved options**



- 1 Shared peripherals, e.g. speaker, display, microphone, should be connected via an approved peripheral sharing device/switch
- 2 CODEC that is not active must be powered-off



# Customer Configurations

- **Periods Processing for Single CODEC**

- **Required when switching between classification levels and between conferences to clear residual information**
- **Data Classification**
  - **On a classified CODEC: audio/video media stream is classified information; other information such as IP Addresses, address book entries, call logs and call data records are sensitive information and could be classified when sufficient information are compiled**
- **Assumptions**
  - **Audio/video media stream is stored/processed on volatile memory during a call**
  - **Environment 1 - CODEC does not store sensitive information on non-volatile memory, e.g. directory services is disabled and not used to store address book entries, call logs and call data records are disabled, etc.**
  - **Environment 2 - CODEC store sensitive information on non-volatile memory, e.g. directory services are used to store address book entries, call logs or call data records cannot be disabled, etc.**





# Customer Configurations

## • Periods Processing for Single CODEC (cont'd)

### – Procedures

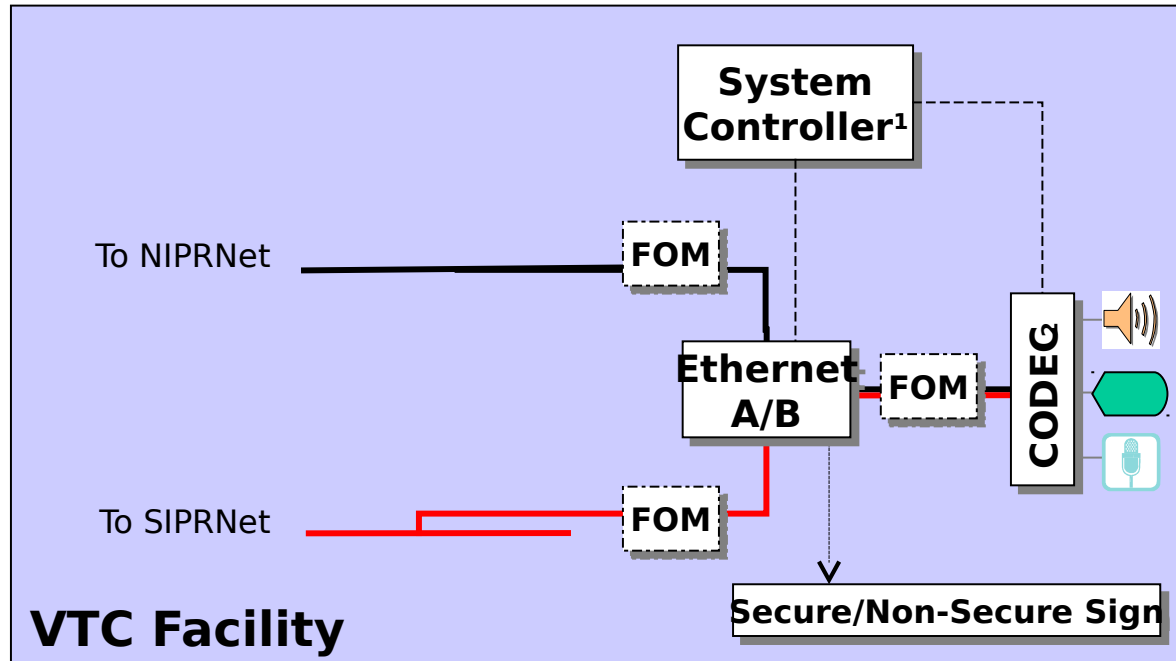
- **Disconnect CODEC from the network to go to transition state**
  - **REMOVE RESIDUAL INFORMATION**
    - For environment 1, power cycle the CODEC to clear residual information on volatile memory
    - For environment 2, clear residual information stored on volatile and non-volatile memory, then reload/reconfigure required information
- Note:**
- **Coordinate with vendor/solutions provider to ensure that all residual information are cleared based on equipment configuration**
  - Remove storage media with different classification level/no-need-to-know information on equipments; equipments with non-removable storage media are not allowed for periods processing
- **Verify that there is NO RESIDUAL INFORMATION on equipments and configure for the new network**





# Customer Configurations

- **Periods Processing for Single CODEC (cont'd)**
  - **Using System Controller**



- 1 **System Controller containing sensitive or classified information to reconfigure the CODEC, e.g. IP Addresses and address book entries, must only be connected to the CODEC during transition state and disconnected at all other times using an approved RED/BLACK disconnect**
- 2 **IP parameters on the CODEC could be automatically obtained from the network DHCP server during restart, eliminating the need to store configuration parameters on the System Controller**



# Customer Configurations

- **Non Open Storage VTC Facility**

- **Lock boxes for SIPRNet wall ports (based on risk analysis of wall port access; enabling port security on the network switch could be an alternate and/or additional mitigation)**
  - **Model No. KL-102 at**  
<http://www.hamiltonproductsgroup.com/GSA/Key.html>
  - **Model No. GL-1259 at**  
[http://www.diebold.com/nasagsa/GSAPhysicalSecurityProducts\\_ControlContainers.htm](http://www.diebold.com/nasagsa/GSAPhysicalSecurityProducts_ControlContainers.htm)
- **Information Processing System (IPS) container for classified equipments, e.g. KIV/KG with crypto key, classified Router, etc.**
  - [https://portal.navfac.navy.mil/portal/page?\\_pageid=181,5004505&\\_dad=portal&\\_schema=PORTAL](https://portal.navfac.navy.mil/portal/page?_pageid=181,5004505&_dad=portal&_schema=PORTAL)
- **Removing crypto key and storing on GSA approved container**  
**Note:** This approach present some issues such as dealing with network alarms, crypto key update, and Router maintenance when the crypto key is removed
- **Additional information for secure storage from the DoD Lock Program**
  - <https://portal.navfac.navy.mil/go/locks>





# Customer Configurations

## • Available Products

| Type                                              | Manufacturer<br>Model Number<br>Estimated Cost | Comments                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Router w/<br>ACL & H.323<br>Firewall <sup>1</sup> | Various                                        | Approved products listed under Technology Type - Firewall at <a href="http://niap-ccevs.org/cc-scheme/vpl/">http://niap-ccevs.org/cc-scheme/vpl/</a> and certain products at <a href="http://niap-ccevs.org/cc-scheme/in_evaluation.cfm">http://niap-ccevs.org/cc-scheme/in_evaluation.cfm</a> |
| IDS <sup>1</sup>                                  | Various                                        | Approved products listed under Technology Type - IDS/IPS at <a href="http://niap-ccevs.org/cc-scheme/vpl/">http://niap-ccevs.org/cc-scheme/vpl/</a> and certain products at <a href="http://niap-ccevs.org/cc-scheme/in_evaluation.cfm">http://niap-ccevs.org/cc-scheme/in_evaluation.cfm</a>  |

- 1 Example products are the Cisco ASA 5500 Series Adaptive Security Appliances/Firewalls, Cisco 4200 Series IDS Sensors, and the integrated Cisco 1841 Router with IOS Firewall and AIM IDS Sensor. For Cisco 1841, Register at <https://www.wwt.com/portalWeb/userSelfReg/begin.do>, Partner Registration Code DVSII0708, then purchase at <https://www.wwt.com/portalWeb/appmanager/maclogin/wwt>**





# Customer Configurations

## • Available Products

| Type                                                                        | Manufacturer<br>Model Number<br>Estimated Cost                                                                                                                                                                                                                                                                                                                                                                     | Comments                                                                                                                |
|-----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| H.460<br>Firewall<br>Traversal<br>Server and<br>Client Proxy<br>Media Relay | Various, examples are:<br>Radvision<br>SCOPIA™ PathFinder™<br>Firewall Traversal - \$xxxx.xx<br>( <a href="http://www.radvision.com">http://www.radvision.com</a> )<br><br>Polycom<br>Polycom V2IU™ Series -<br>\$xxxx.xx<br>( <a href="http://www.polycom.com">http://www.polycom.com</a> )<br><br>Tandberg<br>Border Controller - \$xxxx.xx<br>( <a href="http://www.tandberg.com">http://www.tandberg.com</a> ) | There is currently no NIAP validated devices available, and a waiver is required until the vendor obtain certification. |





# Customer Configurations

## • Available Products

| Type                                | Manufacturer<br>Model Number<br>Estimated Cost                                                                                                                                                                                | Comments                                                                                                                                                      |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Power Controller                    | Various, example is:<br>AMX PC1 - \$250<br>( <a href="http://www.amx.com">www.amx.com</a> )                                                                                                                                   | Required to turn power on/off on the FOM/Transceiver                                                                                                          |
| Fiber Optic Modem/ Transceivers     | Various, examples are:<br>Trendnet TFC-110 - \$59.99<br>( <a href="http://www.trendware.com">http://www.trendware.com</a> )<br><br>Canary CFT-2061 - \$169.50<br>( <a href="http://www.canarycom.com">www.canarycom.com</a> ) |                                                                                                                                                               |
| Ethernet A/B                        | Market Central, Inc<br>5101185 (Desktop)<br>5101186 (Rack mount)<br>\$3,500                                                                                                                                                   | <a href="http://niap-ccevs.org/cc%2Dscheme/st/?vid=1030&amp;maint=156">http://niap-ccevs.org/cc%2Dscheme/st/?vid=1030&amp;maint=156</a>                       |
| Ethernet A/B with System Controller | Various                                                                                                                                                                                                                       | Recommended switches listed at<br><a href="http://disa.dtic.mil/disnvtc/red_black_peripherals.xls">http://disa.dtic.mil/disnvtc/red_black_peripherals.xls</a> |





# Customer Configurations

## • Available Products

| Type                                           | Manufacturer<br>Model Number<br>Estimated Cost | Comments                                                                                                                                                                  |
|------------------------------------------------|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Serial A/B                                     | Various                                        | Recommended switches listed at <a href="http://disa.dtic.mil/disnvtc/red_black_peripherals.xls">http://disa.dtic.mil/disnvtc/red_black_peripherals.xls</a>                |
| A/V Switch<br>for 2 Codec<br>Configuratio<br>n | CIS Secure Computing<br>DTD-DCS-AVS<br>\$3,500 | Available March 2007<br><br>Added Red/Black isolation within the A/V Switch<br>and power-off inactive CODEC                                                               |
| Peripheral<br>Sharing<br>Devices, e.g.<br>KVM  | Various                                        | <a href="https://powhatan.iiie.disa.mil/cap/documentation/index.html#siprnet">https://powhatan.iiie.disa.mil/cap/documentation/index.html#siprnet</a>                     |
| DSN<br>Certified<br>Components<br>, i.e. H.320 | Various                                        | <a href="http://jitc.fhu.disa.mil/certs_reports.html">http://jitc.fhu.disa.mil/certs_reports.html</a> (an account is required to access the list then search for "video") |





# Customer Configuration Checklist

| Configuration Requirements                                                                                                                                                                                                                                                                                                                      | Option 1<br>Single CODEC IP<br>Connection | Option 2<br>Multiple VTC<br>Facilities Video IP<br>Network | Option 3<br>Dial-up<br>Connection |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|------------------------------------------------------------|-----------------------------------|
| Router ACL, Firewall, and IDS protection IAW Network and Enclave STIGs                                                                                                                                                                                                                                                                          | √                                         | √                                                          |                                   |
| Dedicated video LAN separate from the data network                                                                                                                                                                                                                                                                                              | √                                         | √                                                          |                                   |
| Router ACL and Firewall Policy only allow Video-over-IP protocol, i.e. H.323, connection to/from the CODEC <ul style="list-style-type: none"><li>- H.323 Content Based Access Control (CBAC) only allow traffic to/from the CODEC</li><li>- Port security shutdown port on the switch if MAC Address other than the CODEC is detected</li></ul> | √<br><br>√                                | √<br><br>√                                                 |                                   |
| Approved H.460 Firewall Traversal Server placed on the DMZ (for sites that could not upgrade to an H.323 Firewall)                                                                                                                                                                                                                              | √                                         | √                                                          |                                   |
| Approved Ethernet A/B switch for switching between Classified and Unclassified networks on single CODEC solution                                                                                                                                                                                                                                | √                                         | √                                                          |                                   |
| External indicators of secure/non-secure status                                                                                                                                                                                                                                                                                                 | √                                         | √                                                          | √                                 |





# Customer Configuration Checklist

| Configuration Requirements                                                                                                                                                                                                                                                  | Option 1<br>Single CODEC IP<br>Connection | Option 2<br>Multiple VTC<br>Facilities Video IP<br>Network | Option 3<br>Dial-up Connection |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|------------------------------------------------------------|--------------------------------|
| System Controller containing sensitive or classified information to reconfigure the CODEC, e.g. IP Address and address book entries, must only be connected to the CODEC during transition state and disconnected at all other times using an approved RED/BLACK disconnect | ✓                                         | ✓                                                          |                                |
| DSN Certified hardware and/or software designed to send and receive voice, data or video signals, e.g. IMUX, CODEC<br>(<br><a href="http://jitc.fhu.disa.mil/tssi/apl/apl_vtc.html">http://jitc.fhu.disa.mil/tssi/apl/apl_vtc.html</a><br>)                                 |                                           |                                                            | ✓                              |
| Tempest 2/95-A compliant Serial A/B switches and/or Fiber Optic Modems for Red/Black isolation                                                                                                                                                                              |                                           |                                                            | ✓                              |
| Dial isolator for disconnecting dial-in line from the CODEC                                                                                                                                                                                                                 |                                           |                                                            | ✓                              |
| Type 1 encryption for classified connection with established key management procedures                                                                                                                                                                                      | ✓                                         | ✓                                                          | ✓                              |





# Customer Configuration Checklist

| Configuration Requirements                                                                                                                                                                                                     | Option 1<br>Single CODEC IP<br>Connection | Option 2<br>Multiple VTC<br>Facilities Video IP<br>Network | Option 3<br>Dial-up Connection |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|------------------------------------------------------------|--------------------------------|
| Fiber Optic Modem (FOM)/Transceiver powered-off in the path that is not used (Not applicable for Option 3 if using a Tempest compliant Serial A/B switches)                                                                    | ✓                                         | ✓                                                          | ✓                              |
| Non-secure services disabled on the CODEC, e.g. http telnet, and ftp if IP interface is used                                                                                                                                   | ✓                                         | ✓                                                          | ✓                              |
| Periods processing procedures to remove residual information                                                                                                                                                                   | ✓                                         | ✓                                                          | ✓                              |
| Only allowed users can access the CODEC, including protecting access to the CODEC with password                                                                                                                                | ✓                                         | ✓                                                          | ✓                              |
| Disable microphone and cover camera if auto answer is required on the CODEC                                                                                                                                                    | ✓                                         | ✓                                                          | ✓                              |
| CODEC that is not active must be powered-off on dual CODECs solution                                                                                                                                                           | ✓                                         | ✓                                                          | ✓                              |
| Facility authorized for secure VTC (see NSTISSAM TEMPEST /2-95A for RED/BLACK Installation Guidance, and DoD 5220.22-M National Industrial Security Program Operating Manual, Chapter 5 - Safeguarding Classified Information) | ✓                                         | ✓                                                          | ✓                              |





# Customer Configuration Checklist

| Configuration Requirements                                                                                                                                                                                                                                                                                                                                                      | Option 1<br>Single CODEC IP<br>Connection | Option 2<br>Multiple VTC<br>Facilities Video IP<br>Network | Option 3<br>Dial-up Connection |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|------------------------------------------------------------|--------------------------------|
| <b>Dual CODECs</b> <ul style="list-style-type: none"><li>- Shared peripherals should be connected via an approved peripheral sharing device/switch</li><li>- CODEC that is not active must be powered-off</li></ul>                                                                                                                                                             | ✓<br><br>✓                                | ✓<br><br>✓                                                 | ✓<br><br>✓                     |
| <b>On hybrid connections, A/B Switches should be centrally controlled to ensure that both IP and ISDN connections are at the same classification level</b>                                                                                                                                                                                                                      | ✓                                         | ✓                                                          | ✓                              |
| <b>Non-Open Storage VTC Rooms</b> <ul style="list-style-type: none"><li>- Lock boxes for SIPRNet wall ports based on facility risk of unauthorized access</li><li>- Information Processing System (IPS) container for classified equipments, e.g. KIV/KG with crypto key, classified Router, etc.</li><li>- Removing crypto key and storing on GSA approved container</li></ul> | ✓<br><br>✓<br><br>✓                       | ✓<br><br>✓<br><br>✓                                        | <br><br><br>✓<br><br>✓         |



# STIG Configuration Checklist

---

- **Video Tele-conference**
- **Network**
  - **Network Policy, General Perimeter Router, Firewall, IDS, and vendor specific checklist**
- **Security checklists located at**  
<http://iase.disa.mil/stigs/checklist/index.html>





# Connection Approvals

## Order transmission paths:

<https://www.disadirect.disa.mil/products/ASP/welcome.ASP>

- SIPRNet and NIPRNet
- DSN Switched Digital Service
- FTS-2001 ISDN
- Commercial ISDN

## Notes:

- Non-DoD customers that will be using NIPRNet, SIPRNet, and/or DSN need to obtain Joint Staff approval
- For Option 1, backend IP Addresses, i.e. Router internal interface and CODEC IP Addresses will be provided by DISA/DVS.





# Connection Approvals

## Register CODEC on Ports and Protocols Services Management (PPSM) for video-over-IP connection to SIPRNet and NIPRNet

- **PVP - Packet Video Protocol (75)**
  - 1718 TCP/UDP - Gatekeeper Discovery
  - 1719 TCP/UDP - Gatekeeper RAS
  - 1720 TCP/UDP - H.323 Call Setup
  - 1025-65535 Dynamic TCP - H.245 (Call Parameters)
  - 1025-65535 Dynamic UDP - RTP (Video Stream Data) and RTCP (Control Information)
- **TCP (6)/UDP (17) - 53 - DNS Lookup**
- **PPSM Boundaries are:**
  - 12 - Enclave to Enclave DMZ
  - 10 - Enclave DMZ to DOD Network
  - 09 - DOD Network to Enclave DMZ (for calls terminating at a DVS-II Hub or DNS request to the DVS-II DNS Server)
  - 11 - Enclave DMZ to Enclave (for point-to-point calls)
- **PPSM registration is available online at <https://snap.dod.mil/>**
  - After acknowledging "Yes" to continue, select Network (Circuit) Approval Process, then Ports and Protocols Registration, and PnP Registration





# Connection Approvals

## **DSN Certification (of equipments interfacing to the DSN as defined below and currently not on the JITC APL)**

Interoperability and Information Assurance testing of hardware and/or software designed to send and receive voice, data or video signals across a network that provides customer voice, data or video equipment access to the DSN or PSTN, e.g. ISDN CODECs/MCUs, IMUX:

- Complete test submittal
- Coordinate payment of lab testing fees/CRADA agreements
- Provide technical documentation and engineering support
- Configure system according to applicable Security Technical Implementation Guides (STIG)
- Conduct Interoperability and Information Assurance testing
- Attend all in-briefs and out-briefs
- Equipment added to the Approved Products List (APL) at [http://jitc.fhu.disa.mil/tssi/apl/apl\\_vtc.html](http://jitc.fhu.disa.mil/tssi/apl/apl_vtc.html)
- Detailed process description at <http://www.disa.mil/gs/dsn/jic/index.html>





# Connection Approvals

## Video Teleconferencing (VTC) System Certification and Accreditation (C&A):

- Unclassified DVS-G Only – continue to use ATC-R
- Classified/Unclassified DVS-G and DVS-II – requires an ATO from the DAA using DIACAP IAW the latest DoD Policy
- DoD C&A Policy and DIACAP reference are located at <http://iase.disa.mil/diacap/>
- C&A implementation directed by the customer's DAA





# Connection Approvals

## Video Teleconferencing (VTC) System Certification and Accreditation (C&A):

- Army  
DAA:  
DAA Representative(s):  
703-602-7376/DSN 332  
703-602-7395/DSN 332  
Group Email, IACORA@us.army.mil
- Air Force  
DAA: General Senty  
DAA Representative(s):  
AF Network Operations Center/A5  
Information Assurance Manager, CSC  
318-456-7684/DSN 781





# Connection Approvals

## Video Teleconferencing (VTC) System Certification and Accreditation (C&A):

- Navy  
DAA:  
DAA Representative(s):  
Naval Network Warfare Command  
SES, 757-417-6700  
YA-3, 757-417-7911  
YC-3, 757-417-7912
- USMC  
DAA: 703-693-3490  
DAA Representative(s):





# Connection Approvals

## Video Teleconferencing (VTC) System Certification and Accreditation (C&A):

- DISA  
DAA Representative(s):  
703-681-2065

Note: DISA-owned classified/unclassified DVS-G and DVS-II VTC must be included in the DVS-G or DVS-II ATO; call the point of contact for this process at 703-882-2173.





# Connection Approvals

## SIPRNet Connection Approval:

- Provide the following SIPRNet Connection Approval Process (CAP) package:
  - SSAA
  - Statement of Residual Risk
  - Accreditation Letter
  - Connectivity Description Diagram
  - External connections and/or associated operational agreements
  - Consent to Monitor signed by the customer's DAA
  - SIPRNet Connection Questionnaire (SCO) signed by the customer's DAA
- Conduct remote compliance assessment as directed by the SIPRNet Connection Approval Office (SCAO)
- SCAO issue an Authority to Connect (ATC)
- Detailed process description at <https://iase.disa.mil/documentlib.html#siprnetcap>



# Connection Approvals

## NIPRNet Connection Approval:

- SNAP issue an Authority to Connect (ATC)
- NIPRNet connection approval is available online at <https://snap.dod.mil/>
  - After acknowledging "Yes" to continue, select Network (Circuit) Approval Process, and CAP Registration

## DSN Connection Approval:

- SNAP issue an Authority to Connect (ATC)
- DSN connection approval is available online at <https://snap.dod.mil/>
  - After acknowledging "Yes" to continue, select Defense Switch Network, and Submit a New Switch
  - Use Other under Switch Function to specify a CODEC





# Connection Approvals

## DVS Connection Approval:

- Obtain Joint Staff Approval (for Non-DoD access)
- Obtain transmission paths and corresponding ATCs, i.e. SIPRNet, NIPRNet, and/or DSN
- Register for DVS Service
- Complete DD Form 2875 to register site video personnel
- Perform quality assurance testing
- Perform validation testing
- DVS issue an Authority to Connect (ATC)
- Detailed process description at <http://disa.dtic.mil/disnvtc/become.htm>





# CAP Checklist

|                                       | <b>Option 1<br/>Single CODEC IP<br/>Connection</b> | <b>Option 2<br/>Multiple VTC<br/>Facilities Video IP<br/>Network</b> | <b>Option 3<br/>Dial-up Connection</b> |
|---------------------------------------|----------------------------------------------------|----------------------------------------------------------------------|----------------------------------------|
| Order transmission paths <sup>1</sup> | √                                                  | √                                                                    | √ <sup>2</sup>                         |
| Register CODEC Ports and Protocols    | √                                                  | √                                                                    |                                        |
| <b>DSN Certification<sup>3</sup></b>  |                                                    |                                                                      |                                        |
| Conduct interoperability testing      |                                                    |                                                                      | √                                      |
| Conduct Information Assurance testing |                                                    |                                                                      | √                                      |
| Equipment added to APL                |                                                    |                                                                      | √                                      |

## Notes:

- 1 Non-DoD customers using NIPRNet, SIPRNet, and/or DSN need to obtain Joint Staff approval
- 2 Not required for existing dial-up customers that will remain dial-up on DVS-II
- 3 Required for equipments not on the APL that send and receive video on DSN or PSTN





# CAP Checklist

|                                          | <b>Option 1<br/>Single CODEC IP<br/>Connection<sup>1</sup></b> | <b>Option 2<br/>Multiple VTC<br/>Facilities Video IP<br/>Network<sup>2</sup></b> | <b>Option 3<br/>Dial-up Connection<sup>3</sup></b> |
|------------------------------------------|----------------------------------------------------------------|----------------------------------------------------------------------------------|----------------------------------------------------|
| <b>Certification &amp; Accreditation</b> |                                                                |                                                                                  |                                                    |
| Develop SSAA                             | ✓                                                              | ✓                                                                                | ✓                                                  |
| Conduct ST&E                             | ✓                                                              | ✓                                                                                | ✓                                                  |
| Certify and Accredite<br>System          | ✓                                                              | ✓                                                                                | ✓                                                  |
| DAA Issue an ATO                         | ✓                                                              | ✓                                                                                | ✓                                                  |

## Notes:

- 1 Require C&A update to existing VTC facility to include the new IP connection (see major system change requirements on DITSCAP - <http://iase.disa.mil/ditscap/index.html>)
- 2 Require C&A update to the existing network where the Video IP Network will be added (see major system change requirements on DITSCAP - <http://iase.disa.mil/ditscap/index.html>); recommend SSAA Appendix T to accommodate the addition of the Video IP Network
- 3 For existing dial-up customers, only update documentation to indicate transition to DVS-II, e.g. new site ID





# CAP Checklist

|                                       | <b>Option 1<br/>Single CODEC IP<br/>Connection</b> | <b>Option 2<br/>Multiple VTC<br/>Facilities Video IP<br/>Network</b> | <b>Option 3<br/>Dial-up Connection</b> |
|---------------------------------------|----------------------------------------------------|----------------------------------------------------------------------|----------------------------------------|
| <b>SIPRNet Connection Approval</b>    |                                                    |                                                                      |                                        |
| Provide SIPRNet CAP package           | √                                                  | √                                                                    |                                        |
| Conduct remote compliance by the SCAO | √                                                  | √                                                                    |                                        |
| SCAO issue an ATC                     | √                                                  | √                                                                    |                                        |





# CAP Checklist

|                                    | <b>Option 1<br/>Single CODEC IP<br/>Connection</b> | <b>Option 2<br/>Multiple VTC<br/>Facilities Video IP<br/>Network<sup>1</sup></b> | <b>Option 3<br/>Dial-up Connection<sup>2</sup></b> |
|------------------------------------|----------------------------------------------------|----------------------------------------------------------------------------------|----------------------------------------------------|
| <b>NIPRNet Connection Approval</b> |                                                    |                                                                                  |                                                    |
| Complete online NIPRNet CAP form   | ✓                                                  | ✓                                                                                |                                                    |
| NIPRNet issue an ATC               | ✓                                                  | ✓                                                                                |                                                    |
| <b>DSN Connection Approval</b>     |                                                    |                                                                                  |                                                    |
| Complete online DSN CAP form       |                                                    |                                                                                  | ✓                                                  |
| VCAO issue an ATC                  |                                                    |                                                                                  | ✓                                                  |

Notes:

- 1 Only required if requesting a new NIPRNet circuit to the SDN
- 2 Not required for existing dial-up customers that will remain dial-up on DVS-II





# CAP Checklist

|                                                                                              | <b>Option 1<br/>Single CODEC IP<br/>Connection</b> | <b>Option 2<br/>Multiple VTC<br/>Facilities Video IP<br/>Network</b> | <b>Option 3<br/>Dial-up Connection</b> |
|----------------------------------------------------------------------------------------------|----------------------------------------------------|----------------------------------------------------------------------|----------------------------------------|
| <b>DVS Connection Approval</b>                                                               |                                                    |                                                                      |                                        |
| Obtain Joint Staff approval for Non-DoD access                                               | √                                                  | √                                                                    | √ <sup>1</sup>                         |
| Complete transmission path requests and corresponding ATC, i.e. SIPRNet, NIPRNet, and/or DSN | √                                                  | √                                                                    | √ <sup>1</sup>                         |
| Register for DVS-II service                                                                  | √                                                  | √                                                                    | √                                      |
| Perform quality testing                                                                      | √                                                  | √                                                                    | √                                      |
| Perform validation assurance testing                                                         | √                                                  | √                                                                    | √                                      |
| DVS issue an ATC                                                                             | √                                                  | √                                                                    | √                                      |

Notes:

1 Not required for existing dial-up customers that will remain dial-up on DVS-II



